SATELLITE SIGNAL PIRACY

THE EUROPEAN EXPERIENCE

Hackers have repeatedly compromised the satellite-scrambling system commonly used in Europe.

JOHN McCORMAC

SIGNAL PIRATES ARE THREATENING to break the encryption system used by the RCA Digital Satellite System. Hackers, armed with the knowledge gained by breaking VideoCrypt, Europe's similar encryption scheme, are confident that they are close to a break of DSS. (See "Has DSS Been Hacked?" on page 33.) This article outlines the history of the VideoCrypt hack in Europe.

There are three main encryption systems in European satellite TV. The first and most visible is VideoCrypt, used by BSkyB, the broadcaster of Sky and a number of other channels. (BSkyB is the broadcaster of the Sky Multichannels Package, which carries three movie channels and a few general entertainment channels intended for Ireland and the United Kingdom (UK). An estimated 2.5 million subscribers use VideoCrypt smart cards to gain access to programming.

The second principle system is EuroCrypt-M, used by Canal Plus, TV3, FilmNet, TV1000, and a few other programmers. There may be as many as 400,000 subscribers to channels encoded with the EuroCrypt-M scrambling system. The third scrambling system is Nagra Syster, the only one that is still secure from signal hackers. It is used by Premiere, Canal Plus, and Teleclub. While hackers are now actively working on a viable hack for Nagra Syster, the system has fared well during the past four years.

One major difference between Europe and the United States is the uniformity of American laws and their enforcement. Piracy has been able to thrive in Europe because each nation has its own copyright laws, and generally protects only its own channels. This makes it possible, for example, to legally sell pirate smart cards that allow access to VideoCrypt-encoded channels throughout all of Europe, except in the UK.

The VideoCrypt scrambling system used by the DSS system in the United States differs from the European implementation. European VideoCrypt is a purely analog system that scrambles only the video. DSS is a completely digital system that encrypts the digitally encoded video and audio. However, there are many similarities between DSS and European VideoCrypt, including the use of smart cards.

The VideoCrypt scrambling system, like DSS, is based on a secure detachable processor—a removable smart card holds all of the critical information. The smart cards are both the systems' greatest strength and their greatest weakness. Smart cards permit broadcasters to change or upgrade their conditional-access system. In small quantities, an upgrade can be relatively inexpensive, but when the number of cards that have to be replaced increases, so does the cost. For example, BSkyB paid 21 million pounds

www.americanradiohistory.com

for its last card upgrade. Originally, BSkyB planned to issue new versions of smart cards on a three- to six-month cycle to deter hackers. When the cycle grew longer, hackers had enough time to hack the smart cards.

DSS faces a similar threat today. Since the VideoCrypt system in Europe has been totally compromised, European pirates are setting their sights on DSS. Some sources have reported that the DSS system has, indeed, been hacked already, and that pirate smart cards will be on the market as before this article is published. Even if that proves not to be true, European hackers have an intimate understanding of the VideoCrypt system, and they can transfer that knowledge to the DSS digital encryption system.

What Is VideoCrypt?

The European implementation of VideoCrypt is a video-only scrambling system. The active video section of each line is cut and rotated about one of 256 points. The cutpoint for each line is generated from the output of a pseudo-random number generator or PRNG.

The seed for the PRNG is derived from data that is transmitted over the air along with the video. The decoder passes that data to the smart card, which then runs a built-in seed-generation algorithm and returns the correct seed to the decoder. The decoder itself is essentially "dumb" because the main cryptography takes place inside the smart card.

VideoCrypt decoders contain a few built-in algorithms to prevent pirate cards from being used. However due to a programming error on many of the original decoders and IRDs (integrated receiver/descramblers), the most powerful algorithm, the Fiat-Shamir zero-knowledge test, did not work property. Although the same authentication algorithm is used in the DSS system, it is doubtful that the same error was made.

The Fall Of VideoCrypt

VideoCrypt was compromised almost immediately because it contained the same fundamental flaw that was common to most of the smart-card-based systems that were designed in the 1980s: The data flow between the card and the decoder could be tapped just like a phone conversation. The data could then be fed to other decoders, and they could all decrypt programming from data produced by the one authorized card. If the data were sent over a radio transmitter, any decoder equipped with an appropriate receiver could be turned on.

This hack, presented in a article written about the security of smart card based scrambling systems, is known as the McCormac Hack. It works and is still in operation in Spain where it feeds an MMDS (multipoint microwave distribution system) network from one smart card.

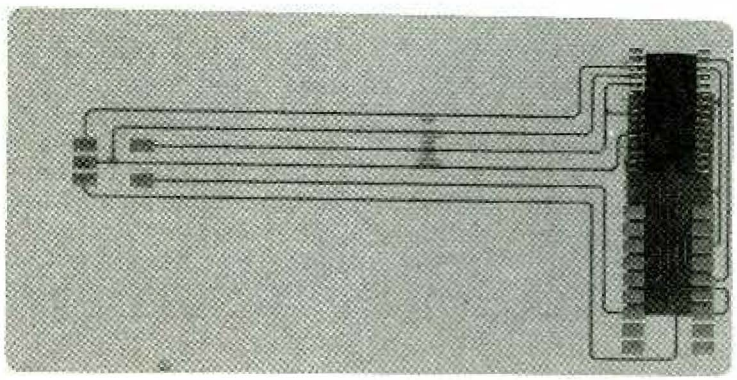
The ease with which VideoCrypt could be hacked was astounding. Here was this system that was advertised as the most pirate-proof system yet developed—yet it was hacked. It was only the beginning of the nightmare for Sky and News Datacom.

Infinite-Lives hack. Another major hack on the security of the VideoCrypt system was called the Infinite-Lives hack. At the time, the smart cards were using EPROM technology and needed a supply of 21 volts DC for programming. By limiting the programming supply to 12 volts DC or so, it was possible to prevent Sky from reprogramming or turning off the cards. (This is a variant of the hack on the France Telecom phone cards whereby the programming voltage pad was covered so that the payphone could not overwrite the card.)

The KENtucky Fried Chip hack. The KENtucky Fried Chip hack was named after Ken Crouch, the head of Sky's Security Department. The hackers had modified the program in the IC that controlled the smart-card interface so that it would read the identity of the smart card inserted in the decoder. It would then look to see if there was a kill message addressed to that particular card and, if there was, the modified chip ensured that the kill message would never reach the card. This technique is known as "chipping" in the United States. It was the first incident of this type of hacking in Europe. In the RCA DSS system, the smart-card interface appears to have a custom microcontroller.

The Ho Lee Fook hack. This hack on VideoCrypt reportedly got its name from the exclamations of executives who learned about it—the hack was a direct replacement for a smart card.

The first version was based on the technology of the KENtucky Fried Chip. It modified the same chip so that it contained the same algorithm embedded in an authorized smart card. Thus the first cardless Sky VideoCrypt decoder was born, a feat that News Datacom claimed was impossible. The VideoCrypt developers had integrated the Fiat-Shamir zero-knowledge test into the system for just such an event. Strangely it never worked.



THIS SMART CARD was used to gain access to VideoCrypt programming.

www.americanradiohistory.com

The first version of the Ho Lee Fook hack proved to be both too insecure and too expensive for pirates. Hackers improved the technique by using low cost PIC microcontrollers manufactured by Microchip Technology.

In early June 1993, the first PIC smart card was developed. This was a genuine pirate smart card—the very thing that VideoCrypt brochures claimed was impossible. This situation lasted for the life of that particular Sky card issue. Sky's VideoCrypt remained completely smashed for approximately one year. All of the Sky channels, the new multichannels, the Adult channel, and TV-Asia were available from the pirates. The minor electronic countermeasures (ECMs) that News Datacom implemented were easily dealt with by hackers. Solutions were available from the hackers sometimes within a few minutes of an ECM.

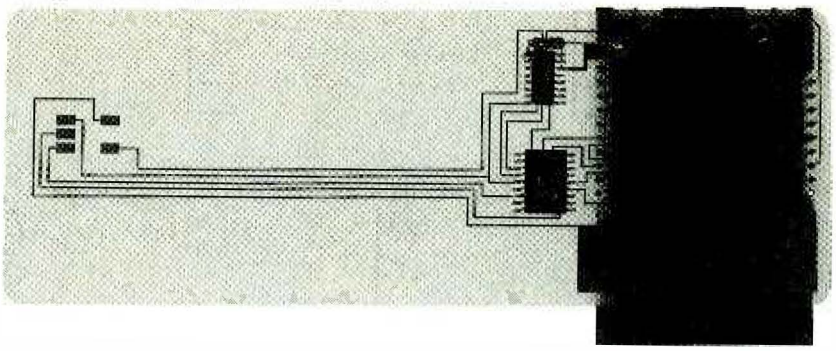
A leap in hacking technology had been made. The newer versions of the pirate cards were reprogrammable. So with a modem, it was possible to serve all the European dealers within a few hours with an update all of their cards.

Because their technical methods had failed to control hacking, Sky and News Datacom sought some help from the law. At first Sky attacked the pirates in the UK but then moved on to Ireland.

A Question of copyright

The laws on piracy are cut and dried in the UK. Fortunately for hackers, Ireland is not part of the UK. A major court precedent was set when Sky tried to pursue David Lyons of Satellite Decoding Systems, an Irish business, through the Irish courts. Sky charged him with copyright infringement of the software in their smart card.

An Irish court granted Sky an Anton Pilar order that allowed company representitives to enter Satellite Decoding Systems' Offaly trading address and seize items or assets that they believed were directly related to the alleged breach of copyright. Sky's intent apparently was to seize the addresses and identities of people who had purchased the PIC cards from satellite Decoding Systems. However, Satellite Decoding Systems did not maintain such records. After months of legal maneuvering and tactical errors, the courts ruled against Sky.



A PHOENIX BLOCKER combines the Phoenix code with a blocker program. The combined program runs on a PIC16C84 microcontroller. The card can turn on all channels on a Sky card and block the kill signal that Sky sens to it.

The TV-Crypt

Perhaps the most significant event of 1994 in the hacking world was the formation of TV-Crypt, a non-commercial group whose interest is to explore scrambling systems. TV-Crypt originated what was called the Season 7 or Omigod hack.

When Sky One was scrambled in September of 1993, many European viewers were cut off watching *Star Trek - The Next Generation*. The seventh and final season of the TV show was to be scrambled and shown on Sky One. Because Star Trek was a favorite show of many hackers, what followed was not unexpected—they put all of their efforts behind a hack.

This time, hackers sought to write an emulation program for their personal computers so that the computer could drive the decoder. Some of the existing commercial hacks were examined and, in one case, the code was extracted from one of the Ho Lee Fook chips. The code for the 8052 microprocessor was transformed into the C language. From there it was transformed into the PC program known as Season Seven or Omigod.

The distribution of the Omigod hack only took a few hours. It was available on all major BBSs and at many Internet sites in Europe. There were even copies floating around at the Cable and Satellite Show in London, one of the biggest trade shows in Europe. Most of the top hackers in Europe were together in the same place at the same time.

Dark Wednesday

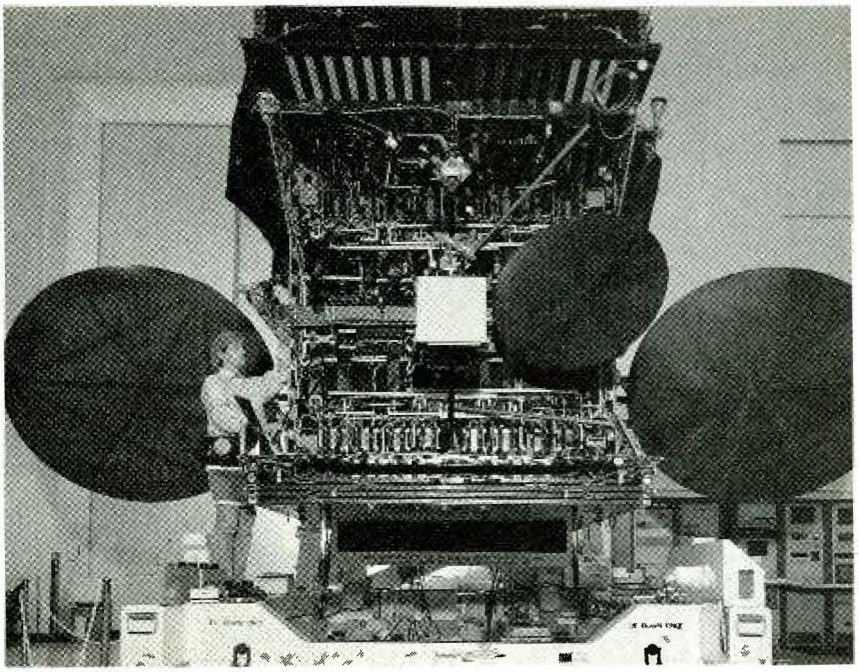
The reality of the situation was beginning to tell on Sky. The company could no longer evade the hacker problem and it switched to its new smart cards, issue 09. Although Sky had been sending these cards out since February, it wasn't until May 18th that the pirate cards ceased to operate. The Omigod program stopped working entirely. Sky had, or so they thought, won the war. To the hackers, the fun had only just begun.

The Great Code Auction

Something decidedly strange happened on June 20th when Sky's 09 code was auctioned at London's Dorchester Hotel. The code was legitimate, and Sky's smart card was compromised again.

It is not known how much money changed hands in the auction, but the theory is that it was in the hundreds of thousands of pounds. Pirates and hackers worked day and night to upgrade their cards based on the auctioned code. They were successful, but only for a week. Then Sky and News Datacom implemented their electronic

www.americanradiohistory.com



HACKERS HAVE SET THEIR SIGHTS on the Hughes HS601 satellite as their next target.

countermeasures that proved to be difficult for the hackers to solve.

The timing of the event had sown the seeds of uncertainty in pirates' minds. Was the auction of the code and the subsequent countermeasures a "sting" by Sky? Was it a pirate operation? The full story of how and why the code was auctioned has not yet been established. There seemed to be so much lying and deception surrounding the code auction that it was difficult to know who was involved.

What followed was a long summer of false starts and disgruntled customers of signal pirates. It seemed that Sky was winning the battle with pirates, as some customers of the pirates were re-signing with Sky. Others customers decided to switch to other program suppliers and watch other channels. Still others decided to buy smart cards from legal outlets and have the cards authorized for only a few weeks, ensuring that they could watch Sky if they wanted to.

The Phoenix hack

The code that had been auctioned in June made its way to the TV-Crypt group where it was analyzed. The code was an improvement over the algorithm of the 07 smart-card issue, but there was something else.

TV-Crypt found that the code could be re-written so that a smart card would generate a correct checksum for any packet of data that it received. Therefore, by using a decoder-emulation program, it was possible to have an authorized smart card treat any data packet sent to it as valid.

That was a significant discovery. Sky's VideoCrypt system operated on an over-the-air authorization procedure. Therefore if a data packet with a correct checksum was sent to a card, it would be possible to switch on cards without the intervention of Sky. The card would not be able to tell the difference between a packet from a decoder emulator program and the real decoder.

By phoning Sky and having the company turn on some legitimate cards over the air, it was possible to build up an image of how the authorization scheme worked. After some analysis of the over-the-air data, some patterns became clear. By the first week in August, the Phoenix program was posted.

To the TV-Crypt group, the Phoenix program was an intellectual exercise to see how the VideoCrypt system worked. There were some pirates, however, who saw it differently and sold the program for, in some cases, thousands of pounds.

The Genesis hack

One of the first commercial hacks based on the Phoenix program was named Genesis, after a Star Trek movie plot. It combined the Phoenix code with a blocker program. The combined program was incorporated in a PIC16C84 microcontroller to create one device that could turn on all channels on a Sky card and block the kill signal that Sky sent to that card.

Sky had totally lost control of its access control system. Even the 09-issue cards that Sky had previously turned off were being reauthorized. Sky and News Datacom were searching desperately for some solution. It seemed that Sky, through its Quick Start scheme, had supplied the pirates with all the genuine Sky cards that they needed. The going price for a Quick Start card in September reached 60 pounds (about $95).

After what can be described as a war of attrition, News Datacom came up with an ECM that completely killed cards activated by the Genesis blockers. The dead cards could not be reauthorized. However, September 1994 was a very bad month for Sky. From pirate sources, who were monitoring the over-the-air data, it became apparent that Sky was trying to kill every card for which it could not account. In that month alone, Sky killed 569,430 cards. It is not clear how many of these were Quick Start cards, or how many people just gave up watching the Sky channels. In October, Sky killed an additional 220,073 cards.

Legal action in the UK

Sky eliminated its security department in March 1993, even though this internal group had succeeded in stemming the flow of piracy in the UK. After

continued on page 76

www.americanradiohistory.com

SATELLITE PIRACY

continued from page 40

that, the company began a deluge of legal action in the UK.

Sky essentially prosecuted the "small guys" who did not have the money to defend themselves. Even though the pirates were breaking the law in the UK, Sky's action was a public-relations nightmare. The company created martyrs.

In one incident, for example, Sky drew the media's attention by trying to prove that one defendant was a main dealer of Genesis blockers. However, that defendant had stocked only 300 blockers—he was certainly not one of the larger dealers.

Sky estimated that it lost 50,000 subscribers and 2.25 million pounds ($3.5 million) to piracy between January 1st and may 18th 1994. However, according to Hack Watch News, a European hacker publication, there were about 300,000 pirate Sky cards in the UK at the beginning of the year.

The 09 issue of cards in February cost Sky approximately 21 million pounds. The next card issue, 0A, that was due in April 1995, probably cost another 21 million pounds

Another card issue (OB) will probably be necessary in November 1995 if Sky wants to maintain the security of its conditional-access system. The present cycle is not short enough to deter pirates from producing their own cards.

The cloning of VideoCrypt

A sure sign that the VideoCrypt scrambling system was thoroughly defeated was that it was cloned. The clone system, called KoyCrypt, was demonstrated at the London Cable And Satellite Show in April 1994. The company that cloned it, Hi Tech Xtravision, also developed a customized smart card that it claimed would be much more difficult to hack. It seemed to be a case of a poacher turned gamekeeper.

Despite the potential benefits of KoyCrypt, broadcasters that want to use it—and perhaps have a more secure system—can't. Copyright issues prevent them from doing so.

The present day

At the time of writing, VideoCrypt is still hacked. There are a few programs available for the PC and the Macintosh that actually allow a computer to tie into a decoder and decode all of the VideoCrypt channels. These programs are free—most of the computer bulletin-board systems in Europe have copies. Today when Sky implements an ECM, the modified versions of the programs are posted on the BBSs within a few hours—an embarrassing situation for News Datacom and Sky.

Many of the pirate smart cards on the market now use pirate technology developed in the U.S. One card has a keypad. When there is an ECM, the pirate card user just telephones an answering service to retrieve a set of numbers. He then enters the numbers on the keypad and the pirate card resumes operation. Another card uses a modem.

Things could change over the next few months though if Sky brings out its new OA-issue card. Then the pirates will be defeated—at least for a little while. However, the problem is that nobody is sure how long the new card will remain unhacked. The most important lesson that the DSS programmers could learn from the European experience is that smart cards have to be changed every six months. Otherwise it's certain that they will be hacked. Ω

HAS DSS BEEN HACKED?

continued from page 36

In practice it is complex. The state of the answer bytes prior to the execution of the nanocommands is known. The process used here is an exhaustive search. The 30h and 03h iterations would be executed exhaustively with all values from 00h to FFh being tried as the input in the 30h loop. The potential for errors exists but it is the simplest way, short of reverse-engineering the card, to obtain the contents of the card memory.

On paper, these steps might look simple. In reality they are complex. The main problem hackers had with the European situation was working out how the recovered data mapped back to standard 6805 commands. Eventually, the op-codes were established and the routines began to make sense. The hackers now have a fully disassembled dump of the ROM and EEPROM of the Sky 09 smart card.

It is probable that the DSS hackers have used the Sky 09 data and knowledge to attack the DSS smart card. The problem for the DSS hackers is knowing the extent and power of the nanocommands in the DSS card. DSS may have a trick or two in its cards to send the hackers back to their drawing boards.

One thing is certain, though. If the DSS engineers do not take into account what happened in Europe, a similar series of events is sure to happen here. Ω

–LEARN ALL THE FACTS–

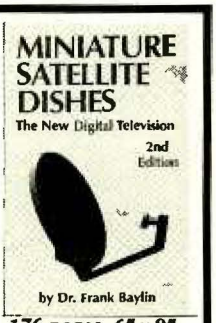
MINIATURE 18" DISHES & HACKING

320 pages, 6" x 8.5"
$50 plus $4 s/h

—TWO NEW BOOKS—
by Frank Baylin / John McCormac

- 18" satellite dish technology, players, programming, encryption and more
- The aclaimed hacker's "bible" outlines all the nitty-gritty technical details

CALL 1-800-483-2423
to order or for a catalog



176 pages, 6" x 9"
$20 plus $4 s/h

Baylin publications
1905 Mariposa, Boulder, Colorado 80302, USA
Telephone: 303-449-4551 FAX: 303-939-8720

www.americanradiohistory.com